Why We Should Put More **Energy** Into **Power Plant Security**

Power plants are a crucial part of any nation's critical infrastructure.

An attack on a power plant could not only have severe economic consequences, but catastrophic environmental and safety ones as well. And even though power plants are safer and more secure today than they ever have been, hacking has also become more sophisticated, reminding us that we must always be on high alert.

Earlier this year a series of cyberattacks on Venezuelan power grids kept the lights off for a full week in some parts of the country. Last summer Russian hackers gained access to the control rooms of several utilities in the U.S.; Russian hackers were also responsible for knocking out Ukrainian power grids in 2015 and 2016. Then there is always the looming risk of physical attacks against power plants and grids by terrorist.

In order to ensure attacks like these never happen again, it is imperative that power plants take the necessary steps to secure the safety and security of their premises, surroundings and personnel.

● **BY** Eifeh Strom, Freelancer

Power Plants Are Still at Risk and Better Security Can Help

Although less vulnerable than before, power plants remain at risk of physical security attacks, as well as other unforeseen dangers.

Ernie Hayden, Founder and Principal, 443 Consulting

Power plants are attractive targets for those looking to create chaos and disrupt national power grids. Adding a robust physical security system has made these facilities less vulnerable, but they still remain at risk.

To truly ensure an effective power plant security program has been implemented, Luke Bencie, Director, and Paige Morrison, Junior Associate, at Security Management International (SMI) suggest adhering to the principles of deter, detect, delay, respond and mitigate.

SMI recommends power companies utilize the CARVER Target Analysis and Vulnerability Assessment Methodology to determine the probability of attack against each critical asset within the system. SMI explained CARVER was originally created by the CIA in the 1970s as a predictive tool to identify where terrorists may strike next. It was revived after the 9/11 terrorist attacks, this time by the private security sector. "Only until you have conducted an assessment can you truly set a baseline for how secure your facility is. CARVER does this for you," they added.

One growing concern at the forefront of the threat landscape relates to the detection and deterrence of drones, or unmanned aerial systems (UAS), according to Darin Dillion, Energy Principal at Convergint Technologies.

In July 2018, the environmental group Greenpeace crashed a Superman-shaped drone into the side of a nuclear

power plant near Lyon, France. The stunt, which caused no damage, was meant to show how vulnerable these facilities are to drone attacks. Currently, technologies related to the detection of UAS are still evolving, as are the written policies and counter measures for UAS deterrence.

Ernie Hayden, Founder and Principal of 443 Consulting also pointed to the threat against Safety Instrumented Systems (SIS), the system that would shut systems down if all personnel were unable to respond to plant calamities. In 2017 the Triton malware (also known as Trisis or HatMan) attack targeted a Saudi petrochemical plant. Hayden explained that this attack disables the SIS of a plant. "By taking the SIS away, this results in the plant operating without automated shutdown capabilities — which could be very dangerous to the plant and to the general population," he said. The malware was discovered again earlier this year.

The precise ways to prevent such modifications to SIS, and therefore prevent future attacks, are still vague. Hayden recommends physical barriers to prevent casual access to the SIS, as well as placing the SIS under "lock and key" and/or posting guards in order to ensure more positive control. Training on-site staff, including vendors and contractors, to ensure they are aware of the threat and aware of the necessity to be more diligent about the threat should also be considered.

▲Critical infrastructure sites now need measures for the detection and deterrence of drones, or unmanned aerial systems (UAS).

Michael Rothschild, Senior Director of Product Marketing at Indegy highlighted how utilities are modernizing power plants and grids to enhance reliability, lower costs and ensure regulatory compliance. "Operational technology (OT) networks are increasingly connected to their IT networks, which together with increased automation increases their attack surface for vulnerability to cyberattacks. Securing automated SCADA generation, transmission and distribution networks from cyberthreats is paramount for improving grid performance and resiliency," he said.

While as a whole countries around the world have continued to step up power plant security, there is still a lot of disagreement as to who is responsible for the overall security of power plants, according to Rothschild.

"Power plants point to the government, yet not all power plants are government run or owned. As a result, the government points back to the plant operators," Rothschild explained. "Due to the interconnected nature of the grid system, its resilience to cyberthreats will only be as strong as its weakest link."

As a result, power, along with other industries considered part of the critical infrastructure sphere, must band together in order to address security vulnerabilities in the system before they are exploited.

Strict Regulations Aim to Keep Power Plants Safe and Secure

Although power plant regulations differ by type and region, they all have the same aim: to ensure the safety and security of the facility.

Power plants are highly regulated due to their importance and vulnerability. Regulations exist for everything, ranging from worker safety to cybersecurity, and can vary depending on the type of power plant.

Nuclear power plants, for example, have higher standards than others since the consequences for any breach, attack or failure is much greater. In the U.S., the Nuclear Regulatory Committee (NRC) is in charge of creating regulations and requirements for nuclear plants in order to make sure they are secure. SMI noted that after 9/11, the

Luke Bencie, Director, Security Management International (SMI).

NRC included more measures for airborne terrorist attacks and actions to reduce radiological release. In terms of cybersecurity, the NRC requires every nuclear plant submit a cybersecurity plan and implementation schedule against threats that could face the plant.

The NRC is also required to conduct "force-on-force" exercises with nuclear power plants every three years, as per the Energy Policy Act of 2005. SMI explained that these security exercises involve having someone attempt to access critical areas of the plants and inflict as much damage as possible. Additionally, the NRC requires that each nuclear plant have an emergency planning zone (EPZ) within roughly a 10-mile radius, and have emergency response exercises every two years. This is then is reviewed by the NRC and FEMA (Federal Emergency Management Agency). Plants must also have plans in place within a 50-mile radius to prevent ingestion of radioactive material.

The primary security standard for those generating electricity in North America is NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection). This series of standards lay out best practices for both cyber and physical security. Even though this is a North American standard, other countries have adopted similar best practices.

In the EU, the Directive on Security of Network and Information Systems (NIS Directive), the first EU-wide cybersecurity legislation, took effect in August 2016. Michael Rothschild, Senior Director of Product Marketing at Indegy explained that the directive establishes minimum security standards for operators of essential services such as the electrical grid. Though it chiefly applies to the EU, anyone dealing with the EU must also comply.

For those power plants not obligated to comply with national standards such as NERC CIP, Ernie Hayden, Founder and Principal of 443 Consulting noted that they are encouraged to follow the United States National Institute of Standards and Technology (NIST) Cybersecurity Framework; this, however, is entirely voluntary. Some power plants may also be encouraged or even directed to follow other security standards such as the International Society for Automation (ISA) standards 62443 for industrial control and automation systems.

When it comes to worker safety, the Occupational Safety and Health Administration (OSHA) in the U.S. has requirements for power plants regarding their health and safety. For example, OSHA requires detector pumps for potential air contaminants that may arise in different types of power plants. OSHA also encourages companies to build on existing safety regulations and create additional company-specific policies, said Luke Bencie, Director, and Paige Morrison, Junior Associate, at Security Management International (SMI).

Unfortunately, a lack of rule implementation can led to fatal incidents, such as the one in Tampa, Florida, in June 2017. SMI explained that Tampa Electric disregarded rules during a maintenance job, resulting in the death of five workers. The company was handed a "willful violation" from OSHA, the most significant violation, along with a fine of over US$100,000.

"Companies should be doing frequent hazard training with employees to ensure they are following the correct safety measures," SMI advised.

It is also important to note that security standards are always evolving due to continued presence of new security threats. As such, existing standards and regulations should be a considered a minimum baseline. Instead, organizations should aim higher and work to stay ahead of future threats.

Deploying the Best Security Solution for Power Plant Protection

Securing power plant facilities requires a comprehensive security solution, including video surveillance, access control and cybersecurity.

Vulnerabilities in power plant security can lead to catastrophic consequences. Deploying the latest security solutions is one way power plants are securing their facilities.

Matthew LaRue, Senior Account Executive, at Convergint Technologies noted that there is a "disruptive digital revolution and digital transformation at hand," resulting from the many software-centric solutions that improve processes, reduce risk, derive savings and enhance overall workflow.

"Many power plants are now seriously considering the various threats to facilities and the available solutions to mitigate threats," LaRue said. Some of the solutions power plants are exploring and implementing include artificial intelligence (AI), advanced analytics, biometrics, data mining and identity access management. These solutions can decipher "real risks" and provide the opportunity for a much more proactive

Matthew LaRue, Senior Account Executive, Convergint Technologies

response, he added.

In terms of more traditional security technologies like video surveillance and access control, there are many ways the latest technologies are assisting with plant security. Ernie Hayden, Founder and Principal of 443 Consulting, noted that improvements in camera technology and deployment capabilities have made it easier to deploy cameras to important areas requiring increased security. Cameras that leverage advanced video analytics and AI are helping plant operators identify threats such as suspicious bags, placement of unusual objects, etc.

Luke Bencie, Director, and Paige Morrison, Junior Associate, at Security Management International (SMI) explained that power plants are also using video surveillance cameras in conjunction with radar. This is because some plants are located near water (as it is used as a coolant), fog and other weather can make surveillance challenging. Since radar senses motion from further away than traditional video surveillance cameras, it is useful in more challenging environments. SMI emphasized that these technologies are to be used in addition to existing video surveillance solutions, not as a replacement for other security measures.

Access control technology is being used by power plants to protect against unwelcome and unauthorized visitors, as well as to monitor who is on the premises at all times. Critical areas of the plant, including the control room, safety systems and others, require card or biometric access, and are sometimes manned by guards.

Darin Dillion, Energy Principal at Convergint Technologies, pointed out that certain technologies installed at utility power plants are used daily to ensure that strict procedures are being followed and compliance is being met. An example might be the use of access control and identity management tools used to track employees, contractors and visitors that enter and exit power plants.

"Access control databases and video files are frequently used to adhere to North American Electric Reliability Corporation (NERC) compliance. Those events and the reporting tools that are output from the respective databases are used for investigations, compliance reporting and for audit purposes," Dillion said.

In addition to secure access management systems, Hayden said some power plants were deploying extra measures like security entrance kiosks to check portable media drives for malware before they are brought inside the power block.

Olea, a manufacturer of security kiosks, offers a portable media cybersecurity kiosk to aid in safeguarding a power plant's networks and incident command systems (ICS) from malware threats due to removable media (e.g., USB drives) brought in by contractors, vendors, employees, etc. The kiosk can scan USB drives and other portable media using up-to-date antivirus systems. "For instance, the kiosk can be placed at the entrance to a production floor, factory building, etc., to specifically ensure that the USB drives are 'clean' before crossing the plant threshold," Hayden explained.

Apart from physical access, power plants must also closely monitor its network access. Michael Rothschild, Senior Director of Product Marketing at Indegy pointed out that there is a large and heterogeneous population of users that have access to the network with credentials and elevated privileges, including employees, subcontractors, partners, suppliers, maintenance workers and perhaps even customers.

"In fact, one of the biggest threats to the security of the network and SCADA operations are these insiders," Rothschild warned. "As such, it is important to give authorized personnel proper training so they know how to minimize risk and appropriate access for their role; no more and no less."

Power Plants Are More Connected, Creating New Cyberthreats

The internet of things (IoT) has been both a blessing and a curse for power plants, as being connected has opened them up to more threats.

The internet of things (IoT) has been a double-edged sword for power plants. On one hand it has offered convenience and more advanced security, but it has also opened the door to threats and attacks that were once not a concern.

Until fairly recently, power plants and SCADA systems were isolated from the rest of the world, said Michael Rothschild, Senior Director of Product Marketing at Indegy. They were not connected to the internet or other systems, making the threat of security incidents very unlikely. Furthermore, the computers used to run industrial processes generally operate for years without any updates or changes.

"The development known as the industrial internet of things (IIoT), has eliminated this buffer zone or 'air gap,'" Rothschild explained. "By connecting once isolated industrial devices to business networks, IIoT has introduced new security risks that could be right out of a science fiction novel. But they're not."

Many rogue factions had specifically targeted critical infrastructure because it is relatively easy and can cause massive amounts of damage, Rothschild said. "We have not seen many catastrophic failures, but there are numerous incidents where proof of concept of attacks have been carried out, e.g., the Ukrainian power outage of 2015, [and] the Rye Brook Dam attack of 2016.

"There are many other incidents where adversaries have gained access to their enemy's critical infrastructure to create a foothold or what we call 'red button functionality' so they can launch an attack at the time of their choosing."

IoT devices such as internet-connected cameras have also been targeted. Many users do not change the default username and password, which makes searching and hacking video feeds quite easy. There are even a number of websites that note devices connected to the internet in important facilities and show their location. The lack of urgency in changing something as simple as a camera password, leaves the entire surveillance system vulnerable.

IoT is also being used to expand sensor arrays such as pressure, temperature and level across power plants, according to Ernie Hayden, Founder and Principal of 443 Consulting. While this may be great for detailed engineering analysis, IoT devices add more traffic to the wireless network and provide more opportunities for attackers to inject malware into the systems. He added that because IoT devices are becoming more prevalent and important to the operation of the plant, they can also be the medium for a denial-of-service (DoS) attack on the plant by shutting down or overwhelming the wireless system.

"Don't forget the Mirai attack of a year ago where an attacker took advantage of flaws in many IoT devices and essentially shutdown a DNS service provider. This event showed that IoT devices need to be tested for security flaws before they are sold/deployed," Hayden reminded.

While IoT has created vulnerabilities, it has also created many opportunities. Matthew LaRue, Senior Account Executive at Convergint Technologies, noted how IoT has also allowed for more efficient energy use — using IoT smart devices has allowed consumers and companies to have improved understanding of energy usage.

Michael Rothschild, Senior Director, Product Marketing, Indegy

When it comes to protecting operational technology (OT) systems from digital security threats, Rothschild explained that it requires the same approach used to protect IT infrastructure. While the tools need to be designed for an OT environment, many of the concepts are the same. This includes: maintaining an up-to-date inventory of assets; patching systems when vulnerabilities are discovered; applying a strong access control standard; deploying a strong, multi-disciplinary threat control system consisting of both signature and anomaly detection; and performing regular device checks on OT assets to ensure they are running as expected and have not been compromised. A&S